## REMARKS

Claims 1-13 and 15-24 are pending in the application. Claims 13 is currently amended. Claim 14 is cancelled. Claims 12 and 23 are indicated to contain allowable subject matter.

Claim Rejections 35 U.S.C. §103

Claims 1-11, 13-15, and 20-22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over United States Patent No. 6,081,793 issued to Challener, United States Patent No. 6,279,109 issued to Brundridge, and further in view of "A Report On Internet Voting." We respectfully traverse the rejection for the reasons explained below.

The Office finds that the teaching of Challener suggests an exclusive execution of program instructions utilizing the smart card . . .'excepting device drivers" is inherent in Challener's execution of program instructions for general purpose voter's PC, see col. 3, lines 60--65" (pages 2-3 of Office action dated February 3, 2004). We respectfully submit that determination is in error and request the Office to reconsider the rejection in view of the remarks below.

At the point where the Challener smart card is engaged, i.e., as noted in col. 3 at lines 60-65, the voter is interacting with the "authentication server 225." Therefore, the smart card is not "for exclusive execution of program instructions found only on the read only storage medium at the voter client during the performance of an election." There is no such exclusivity where the authentication server 225 interacts with the journal server 227 and, as stated in col. 3 at lines 37-39, "[i]n accordance with the present invention, three separate data processing servers collaborate in order to maximize security and privacy throughout the entire voting process." The required collaboration among servers for a particular voting event is evident where the Challener "smart card" merely contains data as depicted in Fig. 2A, such as voter ID, public and private keys, address for precinct, ballot ID of precinct and a PIN for the smart card (see also col. 3 at lines 9-11). Thus, no such exclusive program instructions (or any other program instructions) exist on the smart card as the Office suggests.

The claimed invention as a whole is distinct from Challener where Challener never considered or solved the problem that Applicant has addressed. The entire disclosure of Challener merely refers to the transmission of "data" and never once to

the specific level where program instructions are executed. For example, the program instructions could be contained as "data" in the cryptolope noted by the Office, but the cryptolope is not a read-only storage medium as presently recited in claim 1. If the program instructions are not contained in the Challener cryptolope, then program execution must reside on one or more of the Challener servers, and this is very different from the presently claimed read-only storage.

The Office finds that Brundridge's bootstrap CD may be used to boot the voter client. This would be impossible where the smart card that is relied upon by the Office as the read-only memory does not contain program instructions and merely contains data. The Challener system is basically incompatible with Brundridge where the entire purpose of Challener is to provide security and privacy by non-exclusive processing techniques that require the aforementioned interaction between three different servers. Challener teaches away from a self-booting read only storage medium where the respective servers are required for different levels of security that is imposed over the entire process. This is inapposite to what is presently claimed where a read-only storage medium is configured with program instructions "for exclusive execution of program instructions found only on the read only storage medium at the voter client during the performance of an election," as recited in claim 1.

The motivation to use Brundridge, as asserted in the carryover paragraph on page 3 of the Office action dated February 3, 2004 cannot exist where Challener teaches the desirability of multi-layer security and privacy through three different servers, which leads to the delivery of a cryptolope through non-read-only storage. Incompatibility of different operating systems is not an issue in Challener where the precondition of server interaction with the voter's PC is required to deliver the ballot , the program instructions may be implemented through the various servers, and Challener does not say where the program instructions reside (except to say they do not reside on the smart card).

In summary, the foregoing remarks show that the combination of references, even if indiscriminately combined, do not teach or suggest the claimed limitation of a self-booting read-only storage medium "for exclusive execution of program instructions found only on the read only storage medium at the voter client during the performance of an election." Furthermore, there is no motivation to combine where,

due to the nature of Challener, motivation cannot exist as asserted by the Office because device incompatibility is not an issue, the smart card relied upon by the Office to carry program instructions is shown not to carry program instructions, and Challener does not show the program instructions to be executed at any particular level.

The Office asserts further motivation, namely, that the viruses of "Trojan Horse" software mentioned on page 4 of the California Internet Voting Task force publication may create a serious threat to Internet voting. This passage mentions that "election officials should provide unique operating system and web browser software" for this reason. This is not the purpose of Brundridge where it is merely the case that pre-existing operating systems and programs may be used, for example, where a Windows 95 operating system may be used on a Unix-based PC, or a Windows operating system by be temporarily availed to rum a browser when a NetWare operating system is primarily employed (Brundridge col. 3, lines 30-43). This has nothing to do with unique operating systems that are unique to an election jurisdiction. Furthermore, there is nothing in any of the references that teaches or suggests the particular solution that Applicant has claimed, namely, a self-booting read-only storage medium "for exclusive execution of program instructions found only on the read only storage medium at the voter client during the performance of an election," as recited in claim 1. Even the three references in combination fail to teach or suggest this limitation, and there remains no motivation to modify or combine Challener with Brundridge when Challener continues to teach away from the use of a self booting disk. Again, Challener uses the very different mechanism of multiple server authentication, and is inspecific about where the program instructions are executed.

Claim 22 repeats the limitation as "the read only storage devices containing machine instructions for booting a voter client for exclusive execution of program instructions found only on the read only storage medium at the voter client during the performance of an election, " and so is similarly patentable in like manner with respect to claim 1 Claim 13 has been amended to recite the limitations of former claim 14 where the device drivers are verified to confirm they are not corrupted.

As a whole, the combination of references does not establish a prima facie case for obviousness, and we respectfully request withdrawal of the §103(a) rejection.

Claim Rejections 35 U.S.C §102

Claims 13-19 stand rejected under 35 U.S.C.§102(e) over Brundridge. Claim 13 has been amended to recite the limitations of former claim 14 where the device drivers are verified to confirm they are not corrupted. The Office asserts that the running of "diagnostics" means the verification of device drivers; however, Brundridge merely mentions the use of diagnostics. There is no mention of device driver verification. The assumption by the Office that diagnostics entail driver verification is unwarranted where Brundridge does not specifically teach this is the case and, further, the IEEE dictionary makes it clear that diagnostics pertain to hardware faults, not driver problems (see attached copy of definitions noting particularly "diagnostic.") Thus, Brundridge does not teach or suggest the limitations of claim 13.

Claim Rejections 35 U.S.C §103

Claims 20 and 21 stand rejected under 35 U.S.C §103(a) over Brundridge in combination with "A Report ON The Feasibility of Internet Voting." We respectfully traverse and here assert the previous arguments favoring allowability of claims 1-11, 13-15, and 20-22 *mutatis mutandi*.

## CONCLUSION

For the forgoing reasons, the claims appear to be in allowable condition where the dependant claims contain all of the limitations of the base claims from which they depend and are likewise allowable. Based upon the foregoing discussion, Applicant's attorney submits that the amended claims are allowable and respectfully solicits a Notice of Allowance. Authorization is given to charge deposit account 12-0600 if any additional fees are due.

Respectfully submitted,

Dan Cleveland, Jr., Reg. No. 36,106
Lathrop & Gage L.C.
4845 Pearl East Circle, Suite 300
Boulder, CO 80301
Phone: (720) 931-3012
Fax: (720) 931-3001